Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	CC Docket No. 96-115 RM-11277

REPLY COMMENTS OF CENTENNIAL COMMUNICATIONS CORP.

As explained in its initial comments, Centennial Communications Corp. d/b/a Centennial Wireless and its subsidiaries providing commercial mobile radio service ("CMRS")[1] (collectively "Centennial") make very limited use of customer proprietary network information ("CPNI"). Centennial only uses CPNI to market CMRS calling plans or CMRS features to customers who already purchase CMRS services from Centennial.[2] Even this limited use, however, is currently subject to an array of federal

[1] The subsidiaries joining in this filing are: Bauce Communications of Beaumont, Inc., Bauce Communications, Inc., Centennial Beauregard Cellular LLC, Centennial Beauregard Holding Corp., Centennial Benton Harbor Cellular Corp., Centennial Benton Harbor Holding Corp., Centennial Caldwell Cellular Corp., Centennial Cellular Operating Company LLC, Centennial Cellular Telephone Company of San Francisco, Centennial Cellular Tri-State Operating Partnership, Centennial Claiborne Cellular Corp., Centennial Clinton Cellular Corp., Centennial Hammond Cellular LLC, Centennial Iberia Holding Corp., Centennial Jackson Cellular Corp., Centennial Lafayette Cellular Corp., Centennial Lafayette Communications LLC, Centennial Louisiana Holding Corp., Centennial Mega Comm Holding Corp., Centennial Michiana License Co. LLC, Centennial Michigan RSA 6 Cellular Corp., Centennial Michigan RSA 7 Cellular Corp., Centennial Morehouse Cellular LLC, Centennial Randolph Cellular LLC, Centennial Randolph Holding Corp., Centennial Southeast License Company LLC, Century Beaumont Cellular Corp., Century Cellular Realty Corp., Century Elkhart Cellular Corp., Century Indiana Cellular Corp., Century Michiana Cellular Corp., Century Michigan Cellular Corp., Century Southbend Cellular Corp., Elkhart Cellular Telephone Company, Elkhart Metronet Inc., Lafayette Cellular Telephone Company, Mega Comm LLC, Michiana Metronet Inc., Southbend Metronet Inc.

[2] Using CPNI to market within the same service category does not require customer approval under the Commission's rules. Thus, the debate regarding the appropriate form of customer approval (*i.e.*, opt-in versus opt-out) is not relevant to Centennial's operations and Centennial does not comment on that issue.

and state privacy laws and regulations that require Centennial, among other things, to ensure the proper handling of CPNI. In addition, Centennial has a very strong business interest in protecting its customers' CPNI.

As a result, Centennial takes its responsibility to protect CPNI very seriously. For example, after reading press reports that data brokers were illicitly obtaining CPNI, Centennial's President, Phillip H. Mayberry, sent a memorandum to all Centennial employees explaining the reported activities of the data brokers, and reminding them of Centennial's Code of Conduct privacy policies and that Centennial supervisors are available to answer any questions employees may have. Clearly, the existing rules, combined with Centennial's own business interests, have provided the right incentives for Centennial to implement a policy of vigilance in the protection of CPNI. In fact, most of the commenters participating in this proceeding agree with Centennial, that more rules—and particularly those proposed by the Electronic Privacy Center ("EPIC")—will do very little if anything to combat the use of pretexting by data brokers or others to improperly obtain CPNI.

I. ADDITIONAL RULES WILL NOT SOLVE THE PRETEXTING PROBLEM

EPIC has proposed additional "safeguard" rules for CPNI, such as mandatory passwords, audit trails, encryption and disclosure notices. Most commenters agree with Centennial that these proposed additional measures are, for the most part, solutions in search of a problem. The proposals either fail to strengthen carriers' defenses against the illicit behavior being addressed in this proceeding—pretexting—or they are overly burdensome while offering little to no protection against that illicit behavior. Even some of the state public utility commissions that filed comments recognized that many of the

proposals fail to address pretexting or are disproportionately burdensome or otherwise harmful. For example, The Public Service Commission of Missouri recognizes that requiring passwords, audit trails, encryption and disclosure notices will have little if any effect on preventing pretexting.[3] The Public Utilities Commission of Ohio argues that limiting data retention may run afoul of state data retention requirements, while simultaneously frustrating customers' and law enforcement's legitimate uses of CPNI.[4] Moreover, the United States Departments of Justice and Homeland Security also urge the Commission not to adopt the proposal to require the destruction of call records, which would result in the "sacrificing [of] lawful access to important information that helps solve crimes, prevent terrorist attacks, and safeguard our national security."[5]

Carriers, who have the best understanding of the impact the proposals would have on the industry, have all pointed out that the various proposals largely bear no relationship to pretexting, and even when relevant to pretexting, report that they are overly burdensome in proportion to the small benefits they would bring, if any. For example, the other carrier commenters agree with Centennial that encryption of databases storing CPNI would only be useful if the data brokers obtain their information by hacking into such databases, and there is nothing in the record suggesting that this is the case.[6] As suggested in the Commission's NPRM, encryption of stored data is "***essentially***

---

[3] Comments of the Public Service Commission of the State of Missouri, at Section II A-C, E (hereinafter "Missouri PSC Comments").

[4] Comments of the Public Utilities Commission of Ohio, at 14-17.

[5] Comments of the United States Departments of Justice and Homeland Security at 2 (hereinafter "DOJ/DHS Comments").

[6] Qwest Comments at 12; CTIA—The Wireless Association Comments at 15 (hereinafter "CTIA Comments"); Comments of Dobson Communications Corporation at 8 (hereinafter "Dobson Comments"); Comments of Rural Cellular Association at 4; Comments of Sprint Nextel Corporation at 13-15; Comments of Time Warner Telecom at 15 (hereinafter "Time Warner Telecom Comments").

unrelated to protecting against inappropriate disclosure of CPNI."[7] It is the inappropriate disclosure of CPNI that is being addressed in this proceeding, not hacking. EPIC's encryption proposal is plainly inappropriate and unwarranted.

Moreover, other carriers agree with Centennial that current industry practices provide for sufficient "audit trail" information (such as the date and time a customer's account was accessed, why it was accessed and any action taken) to assist carriers and law enforcement in combating pretexting.[8] This is particularly true given that even the most detailed audit trail records will not reveal the pretexter's true identity, because the "trail" will simply reflect that customer service representative believed (based on customer identification methods) that he or she was disclosing the CPNI to the customer. Customer service records, therefore, can only give limited circumstantial information such as date and time of contact by the purported customer. Notably, nowhere in the joint comments filed by the United States Departments of Justice and Homeland Security did those government agencies complain that carriers' current "audit trail" procedures are lacking or have otherwise hindered their law enforcement efforts.[9]

The proposed requirement to notify customers in cases of unauthorized access or disclosure, as well as in cases of permissible access/disclosure, has been similarly criticized by commenters. Codifying a post-breach requirement in federal regulations would be quite difficult given that the particular form and content of such notices will vary considerably depending on who improperly accessed the CPNI and the particular

---

[7] *In Re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information,* Notice of Proposed Rulemaking, 21 FCC Rcd 1782 at ¶ 19 (FCC rel. Feb. 14, 2006) (emphasis added) (hereinafter "NPRM").

[8] *See e.g.,* Comments of Verizon at 13; Qwest Comments at 13-15; CTIA Comments at 14.

[9] DOJ/DHS Comments.

circumstances involved. For example, a notice in a situation where an affiliate was inadvertently given access to CPNI without customer approval but the affiliate never used the information would be quite different from a notice in a situation involving access by a pretexter. Moreover, certain states have their own post-breach notice requirements, which are likely to differ and would have to be reconciled with any federal requirement. Given the lengthy process that would be involved and that Congress is still considering a number of bills all proposing post-breach CPNI notices,[10] the Commission should refrain from adopting any post-breach notice requirements.

As for notices in cases of permissible access/disclosure, the sheer number of notices that would be required makes such a proposal unmanageable and tremendously burdensome. Dobson Cellular, for example, estimates that under such a requirement it would have to "generate at least ***35,000-45,000 notices*** to its customers ***per day*** based on the average number of inquiries handled by its customer service, with most if not all involving accessing or disclosing CPNI."[11] Worst of all, customers are very likely to be confused by receiving frequent notices from carriers disclosing lawful access/disclosure, which in most cases would have been spurred by the customer's own call to the carrier.

Finally, many commenters, including The National Association of State Utility Consumer Advocates ("NASUCA"), find that passwords are of limited use in protecting consumers' CPNI—principally because consumers fail to use them properly.[12] NASUCA points out that consumers either forget their passwords, use the same passwords for multiple accounts, or often lose their passwords, which requires companies

[10] H.R. 4943, H.R. 4662 and S. 2389.
[11] Dobson Comments at 7 (emphasis added).
[12] *See e.g.,* Comments of the National Association of State Utility Consumer Advocates at 15-17 (hereinafter "NASUCA Comments"); Missouri PSC Comments at Section II.A; Time Warner Telecom Comments at 12; Comments of US LEC Corp. at 3; Verizon Wireless Comments at 8-9.

to have replacement procedures that can provide pretexters with an opportunity to access the account.[13] Many customers use easily guessable passwords, such as words occurring in the dictionary or the name of a pet or child. There are also inherent flaws with many password mechanisms. "Secret" biographical information used to obtain replacements for forgotten passwords, such as mother's maiden name or social security number, can sometimes be found on the Internet and used to obtain the customer's password. Other commenters agree with Centennial that the majority of consumers find passwords burdensome and annoying.[14] Centennial already offers customers the option of protecting their accounts through a password but rarely do customers establish one.[15] The Commission should not force consumers to use passwords when most of them have rejected such measures, and often fail to even use passwords safely.

II. A SAFE HARBOR WOULD ENCOURAGE VIGILANCE

Centennial strongly supports the suggestion of several commenters to create a safe harbor mechanism.[16] The idea behind safe harbor mechanisms is to reward carriers who go above and beyond prescriptive rules and to motivate companies to establish and practice the highest level of institutional vigilance. For example, Centennial would support annual training sessions; company-confidential, written customer verification procedures; posting of plain-language privacy policies on a carrier's website; and, despite the limitations of passwords, offering customers the option of password protection as elements of a safe harbor mechanism. Creating such a mechanism would give carriers

[13] NASUCA Comments at 15-17.
[14] Comments of Cingular Wireless LLC at 19; Verizon Wireless Comments at 9. *See also* Comments of Charter Communications, Inc. at 25-26.
[15] Dobson Cellular notes that although it offers its subscribers the ability to protect their accounts through the use of passwords, that only 10% of its subscribers have chosen to do so. Dobson Comments at 6. BellSouth also offers its customers the option of using a password to protect their accounts. Comments of BellSouth Corporation at 16.
[16] Comments of Cingular Wireless LLC at 30; Verizon Wireless Comments at 20.

additional incentives to increase their efforts to protect CPNI, and give consumers additional tools in fighting pretexting.

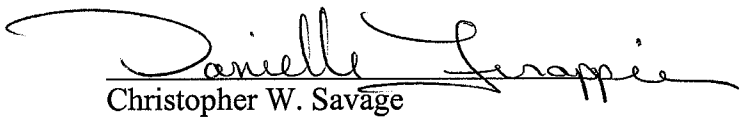
At the same time, a safe harbor mechanism would properly recognize that despite best efforts, no amount of rules and procedures aimed *at carriers* can thwart each and every time the *fraudulent conduct of third parties*. Carriers who can demonstrate a high level of commitment to protecting the privacy interests of customers should not be held to the impossible standard of outmaneuvering the pretexters with 100% accuracy when no one (including EPIC) claims to fully understand the methods used by pretexters, and when those methods are likely to evolve over time.[17]

III. CONCLUSION

The real solution to pretexting lies in continued enforcement of the current CPNI rules, and increased vigilance and cooperation between industry and regulators. None of the commenters in favor of EPIC's proposals have shown that the proposed rules would help combat pretexting. This is not surprising since, as Centennial pointed out in its initial comments, the proposals largely fail to even address pretexting. Where the proposals arguably do address it, they suggest codifying static "solutions" in a constantly morphing security environment. While adopting EPIC's proposals may create the illusion that "something is being done" about pretexting, the comments submitted in this proceeding amply demonstrate that the Commission's and industry's resources would be put to better use in working together to combat the wrongdoers—the pretexters—rather than saddling industry with ineffective regulatory requirements.

[17] Comments of The Electronic Privacy Information Center *et al.* at 5-6; NPRM at ¶¶ 10-11.

Respectfully submitted,



Christopher W. Savage
Danielle Frappier
Cole Raywid & Braverman, LLP
1919 Pennsylvania Ave., NW, Suite 200
Washington, D.C. 20006
(202) 659-9750
csavage@crblaw.com; dfrappier@crblaw.com

Counsel for Centennial Communications Corp.

William Roughton
Vice President, Legal and
Regulatory Affairs
Centennial Communications
Corp.
Of Counsel

June 2, 2006